образования, которые будут иметь важное значение для систем ЭО на период до 2015 года.

1. American Society for Technology and Development (ASTED), http://www.astd.org
2. Усков В.Л., Иванников А.Д., Усков А.В. Качество электронного образования // Научно-технический и научно-производственный журнал «Информационные технологии». – М.: Изд-во «Информационные технологии», №3, 2007. С. 36-43.

Усков В.Л., Усков А.В., Иванников А.Д.

КОНЦЕПТУАЛЬНАЯ И АРХИТЕКТУРНАЯ МОДЕЛИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ ОБРАЗОВАТЕЛЬНЫХ СЕТЕЙ

uskov@bradley.edu
Бредли университет
г. Пеория

Вступление.

Задача создания компьютерной сети отдельной образовательной организации (колледжа, университета) в пределах одного здания может быть решена относительно легко. Однако, инфраструктура современных образовательных организаций (например, таких как, крупные университеты, колледжи, ассоциации университетов и колледжей, виртуальные университеты, корпоративные университеты глобальных компаний) может включать в себя многочисленные географически распределенные департаменты (факультеты, колледжи, кафедры, научные центры и лаборатории, филиалы, представительства, центры повышения квалификации и переподготовки кадров, и т.п.) самой образовательной организации, а также десятки тысяч студентов, слушателей, аспирантов, научных работников, преподавателей, совместителей, и др. Например, статистические данные об инфраструктуре российского мега-университета - Московского государственного университета экономики, статистики и информатики (МЭСИ) - таковы [1]: 6 институтов, 21 учебный центр, техникум, колледж, 170 тысяч обучаемых, 50 филиалов в России, 4 филиала за рубежом, 120 представительств, десятки серверов университетского уровня администрирования, сотни серверов в подразделениях университета, десятки тысяч пользовательских компьютеров (настольных, переносных, портативных). Единственным средством информационного объединения всех структурных подразделений образовательной организации такого типа и людских ресурсов является создание корпоративной образовательной сети (КОС).

Несмотря на интенсивное внедрение вновь создаваемых технологических решений в области информационной безопасности (ИБ) КОС, уровень криминогенности в информационной сфере в ведущих образовательных организациях

мира постоянно повышается, что приводит к значительным финансовым потерям. Например, согласно докладу компании Computing Market Intelligence [2] на основе опроса более 60 ведущих корпораций США, среднестатистические финансовые потери в год от одного компьютера, использующего операционную систему Windows и допустившего проникновение вредоносных кодов (ВК) разных типов, могут составлять от 281 до 340 долларов США. С другой стороны, результаты опроса более 35 крупных организаций США, проведенного корпорацией PGP в ноябре 2007 года [3] по выявлению финансовых потерь от несанкционированного доступа к конфиденциальной информации и ее неправомерному использованию, показывают, что в 2007 году а) финансовые убытки от потери информации (файла данных) только об одном сотруднике организации составили в среднем 197 долларов США (для сравнения, в 2006 году – 182 доллара США), б) суммарные финансовые потери от одного инцидента, связанного с несанкционированным доступом к корпоративным базам конфиденциальных данных, чтением или неправомерным копированием конфиденциальной информации, составили 6.3 миллиона долларов США (для сравнения, в 2006 году – 4.8 миллиона долларов). При условии, что в средней по размеру образовательной организации могут обучаться десятки тысяч студентов и работать несколько тысяч преподавателей, аспирантов и административных работников, финансовые потери от нарушения ИБ КОС могут исчисляться миллионами долларов США в год.

В связи с этими и многочисленными другими докладами и фактами, можно с уверенностью утверждать, что проблема надежной защиты корпоративных образовательных сетей является одной из наиболее актуальных и значимых для современных образовательных организаций. Результаты опроса 592 университетов и колледжей США, проведенного в ноябре 2007 года ассоциацией EDUCAUSE [4], убедительно показывают, что вопросы информационной безопасности КОС и ее баз данных, а также контроля за доступом в КОС, в 2006-2007 годах являлись вопросам первостепенной важности для администрации университетов-респондентов и останутся приоритетными вопросами на ближайшую обозримую перспективу.

Анализ моделей информационной безопасности КОС крупных университетов и университетских ассоциаций мира, корпоративных университетов и отдельных корпораций позволяет сформулировать концептуальную модель ИБ КОС крупной образовательной организации; основные положения разработанной концептуальной и архитектурной моделей приводятся ниже.

Концептуальная модель ИБ КОС.

Руководящие документы в области ИБ являются основой успешной ИБ КОС [5]. Иерархическая модель документов ИБ КОС должна включать: 1) стратегию ИБ КОС (самый верхний уровень), 2) политики ИБ, 3) стандарты ИБ, 4) технологии ИБ, 5) процедуры и мероприятия ИБ (низший уровень).

Жизненный цикл системы ИБ КОС описывается спирально-эволюционной моделью, компонентами которой являются следующие последовательные этапы:

1. оценка возможных рисков и угроз для ИБ КОС,
2. разработка новых или модификация существующих политик и технологий ИБ,
3. разработка процедур и мероприятий по защите ИБ КОС, включая а) превентивные средства и мероприятия, б) детективные средства и мероприятия обнаружения атак вредоносных кодов (АВК) и их удаления или обезвреживания во всех компонентах КОС,
4. обучение всех видов пользователей КОС разработанным политикам, стандартам, технологиям, процедурам и мероприятиям ИБ КОС,
5. аудит и мониторинг ИБ КОС,
6. немедленное реагирование на обнаруженные АВК и их отражение,
7. восстановление нормальной работоспособности КОС в целом и отдельных ее компонентов в случае успешной АВК.

Участниками системы КОС являются следующие группы пользователей с существенно различными приоритетами (уровнями) доступа как в КОС в целом, так и к отдельным компонентам КОС:

- ВР - высшее руководство образовательной организации, т.е. ректор, проректоры, члены совета попечителей организации,
- РП - руководители крупных подразделений организации, т.е. деканы факультетов, директора центров, филиалов и представительств, начальники служб и подразделений,
- РБ - руководители служб всех типов безопасности организации,
- СА - разработчики КОС, провайдеры отдельных компонентов КОС и ее системные администраторы (в общем случае, указанные 3 типа участников КОС могут быть представителями трех совершенно разных организаций; например, при использовании коммерческой системы управления электронным обучением сама система может физически находиться на серверах ASP-провайдера, а не на серверах университета; однако, для простоты изложения, ниже считается, что представители всех трех указанных групп участников КОС являются представителями одной и той же образовательной организации);
- ПР - преподаватели и разработчики образовательного контента (в общем случае, указанные 2 типа участников КОС могут быть представителями двух совершенно разных организаций, например, при использовании коммерческого образовательного контента в КОС, разработанного вне образовательной организации; однако, для простоты изложения, ниже считается, что представители двух указанных групп участников КОС являются представителями одной и той же образовательной организации);

- СС - студенты, аспиранты и сторонние пользователи КОС (в общем случае, следует различать указанные группы участников КОС по приоритету их доступа в КОС, к ее отдельным приложениям, к модификации данных в КОС, к скачиванию образовательной информации из КОС, и т.п.; однако, для простоты изложения, ниже считается, что представители трех указанных групп участников КОС являются представителями одной образовательной организации).

Архитектурная модель управления ИБ КОС.

Архитектурная модель управления ИБ КОС образовательной организации является неотъемлемой частью концептуальной модели ИБ КОС. Она должна включать в себя несколько иерархических уровней управления ИБ КОС, каждый из которых, в свою очередь, включает в себя как превентивные (т.е. до обнаружения АВК) мероприятия, так и детективные (т.е. после обнаружения АВК или их результатов) мероприятия. Уровни архитектурной модели включают а) административный (высший уровень), б) технический (т.е. уровень пользовательских компьютеров – офисных, домашних, переносных, в учебных лабораториях и исследовательских центрах), в) физический (т.е. физическую охрану компьютерных лабораторий, серверов, и т.п.), г) сетевой (т.е. уровень распределенной компьютерной сети), д) информационный (т.е. уровень данных и информации в КОС) уровни. Основные компоненты разработанной архитектурной модели КОС - уровни управления ИБ КОС, конкретные мероприятия по обеспечению ИБ КОС и вовлеченность в них различных участников КОС - приведены ниже в Таблице 1.

Таблица 1.
Уровни управления ИБ КОС и вовлеченность
разных участников КОС в мероприятия по обеспечению ИБ

Уровни управления КОС и отдельные мероприятия по обеспечению информационной безопасности КОС		Вовлеченность участников в мероприятие ИБ					
		ВР	РП	РБ	СА	ПР	СС
Административный уровень							
Превентивные средства		ВР	РП	РБ	СА	ПР	СС
1	Стратегия, отдельные политики ИБ, стандарты, технологии и мероприятия по обеспечению ИБ	X	X	X			
2	Правила использованием КОС в образовательном процессе	X	X	X	X		
3	Оценка возможных рисков и угроз для ИБ	X	X	X	X		
Детективные средства		ВР	РП	РБ	СА	ПР	СС
1	Немедленное реагирование на обнаруженные АВК и их отражение		X	X	X	X	X
2	Восстановление нормальной работоспособности КОС в целом и отдельных ее компонентов в случае успешной АВК		X	X	X	X	X
3	Анализ причин успешной АВК и разработка новых или модификация существующих	X	X	X	X	X	X

Уровни управления КОС и отдельные мероприятия по обеспечению информационной безопасности КОС		Вовлеченность участников в мероприятие ИБ					
		ВР	РП	РБ	СА	ПР	СС
	тик, технологий, процедур и мероприятий ИБ						
4	Аудит ИБ КОС на предмет отражения в будущем обнаруженной успешной АВК		X	X	X		
Технический уровень (уровень пользовательских компьютеров)							
Превентивные средства		ВР	РП	РБ	СА	ПР	СС
1	Контроль доступа пользователей в КОС в целом и к ее отдельным компонентам			X	X		
2	Конфигурирование пользовательских компьютеров			X	X	X	X
3	Защищенность компьютеров от АВК			X	X	X	X
4	Использование межсетевых экранов			X	X	X	X
6	Контроль источников информации и генераторов данных в КОС				X	X	
6	Шифрование передаваемой пользовательской информации и данных				X	X	X
7	Сканирование пользовательских компьютеров на предмет обнаружения в них уязвимостей в смысле потенциальных АВК				X	X	X
8	Немедленная установка всех вновь появляющихся от компаний-производителей программных усовершенствований (updates) или «заплаток» (patches) на системное (операционная система) и прикладное (пакеты программ) программное обеспечения пользовательских компьютеров				X	X	X
Детективные средства		ВР	РП	РБ	СА	ПР	СС
1	Немедленное оповещение пользователей об обнаружении АВК или несанкционированном доступе				X		
2	Обнаружение и исправление результатов несанкционированных вторжений и АВК и их уничтожение				X	X	X
3	Обеспечение целостности и конфиденциальности информации (файлов) пользователей на их компьютерах				X	X	X
Физический уровень							
Превентивные средства		ВР	РП	РБ	СА	ПР	СС
1	Правила и часы использования компьютерных учебных и исследовательских лабораторий и центров, центров создания образовательного контента, офисов, серверных центров, и т.п.	X	X	X	X	X	X
2	Закрываемые на ключ (электронный или ческий) и находящиеся под охраной терные учебные и исследовательские	X	X	X			

Уровни управления КОС и отдельные мероприятия по обеспечению информационной безопасности КОС		Вовлеченность участников в мероприятие ИБ					
		ВР	РП	РБ	СА	ПР	СС
	рии и центры, офисы, библиотеки, и т.п.						
3	Физическая защита компьютеров и периферийных устройств (например, принтеров, сканеров, видео камер, и т.п.) в лабораториях с использованием специальных кабелей, замков, датчиков, и т.п.	X	X	X			
4	Дистанционное видео наблюдение (слежение) и запись событий на видеокамеры	X	X	X			
5	Климатический контроль (температура, влажность)	X	X	X			
6	Противопожарные средства	X	X	X			
7	Физическая защита электрических кабелей, экранизация электромагнитных наводок.	X	X	X			
8	Патрулирование компьютерных центров и лабораторий (особенно, в ночное время)	X	X	X			
Детективные средства		ВР	РП	РБ	СА	ПР	СС
1	Средства немедленного оповещения о возможной краже оборудования КОС		X	X			
2	Тщательный мониторинг компьютерных учебных и исследовательских лабораторий и центры, библиотек, и т.п. на предмет возможных повторных краж оборудования КОС		X	X			
Сетевой уровень							
Превентивные средства		ВР	РП	РБ	СА	ПР	СС
1	Контроль доступа в КОС			X	X		
2	Шифрование передаваемой информации и данных			X	X		
3	Сканирование КОС на предмет обнаружения уязвимостей для потенциальных АВК и несанкционированного доступа			X	X		
4	Использование межсетевых экранов			X	X		
5	Создание и активное использование виртуальных частных сетей VPN в КОС			X	X		
6	Мониторинг регистраций (логов) в КОС			X	X		
7	Мониторинг и анализ траффика КОС в целом и отдельных ее подсетей			X	X		
8	Методика создания паролей (логинов) для входа в КОС и частоты смены паролей			X	X		
Детективные средства		ВР	РП	РБ	СА	ПР	СС
1	Немедленное оповещение о потенциальных АВК или несанкционированном вторжении в КОС			X	X		
2	Обнаружение и исправление результатов несанкционированных вторжений и АВК			X	X		

Уровни управления КОС и отдельные мероприятия по обеспечению информационной безопасности КОС		Вовлеченность участников в мероприятие ИБ					
		ВР	РП	РБ	СА	ПР	СС
3	Анализ регистраций (логов) в КОС			X	X		
4	Мониторинг основных помещений организации с расположенными в них центральными серверами КОС, дистанционное видео наблюдение (слежение) и запись на видеокамеры информации о всех входящих, выходящих и работающих сотрудниках КОС, и			X	X		
Информационный уровень							
Превентивные средства		ВР	РП	РБ	СА	ПР	СС
1	Контроль доступа в КОС			X	X		
2	Авторизация доступа в КОС и ее использования		X	X	X		
3	Управление модификацией и изменением данных и информации в КОС по их типу, стандартам, протоколам и назначению; обеспечение полной совместимости новых и			X	X		
4	Шифрование информации и данных в КОС на основе разнообразных криптографических алгоритмов, стандартов и протоколов			X	X	X	X
5	Управление системой пользовательских приоритетов доступа к данным и информации в КОС и их возможным изменениям			X	X	X	X
6	Контроль источников изменения информации и генераторов данных в КОС				X	X	X
Детективные средства		ВР	РП	РБ	СА	ПР	СС
1	Анализ регистраций (логов) в КОС			X	X		
2	Распределение обязанностей по хранению, мониторингу изменений данных и информации в КОС и ее компонентах			X	X	X	X

Следует особо подчеркнуть, что практические реализации разработанной архитектурной модели по обеспечению ИБ КОС могут существенно отличаться друг от друга в зависимости от:

1. масштаба образовательной организации и размеров ее КОС, т.е. от количества ее студентов, аспирантов, преподавателей, администраторов, инженерно-технических работников, обслуживающего технического персонала, подсетей КОС, используемых каналов связи с подразделениями, и т.п.),
2. структурной модели образовательной организации, например, а) отдельный университет или колледж, б) организация с центральным отделением (университетом) и многими географически распределенными ее подразделениями (кафедрами, филиалами, обучающими центрами, и т.п.), в) ас-

социация географически распределенных университетов или колледжей без центрального отделения (университета), и др.,
3. доступного объема финансирования работ по обеспечению ИБ КОС,
4. степени использования а) коммерческих продуктов третьих сторон, б) провайдеров Интернета, беспроводной сети, серверов вне пределов образовательной организации, в) аутсорсинга используемых программных приложений и образовательного контента КОС, технологий ИБ, и т.п.

Заключение.

Разработанные и описанные выше концептуальная и архитектурная модели по обеспечению информационной безопасности корпоративной образовательной сети крупной образовательной организации (с тысячами пользователей внутри сети КОС и за ее пределами, тысячами пользовательских компьютеров в лабораториях организации, десятками центральных серверов и серверов отдельных подразделений , и более, чем 20 подсетями в составе КОС) успешно прошли всестороннее тестирование в одном из крупных университетов и активно используются, начиная с октября 2005 года. За это время выявлена 1 успешная АВК, связанная с небрежным обращением с паролем одного из администраторов организации, и 4 инцидента, связанные с попытками неправомерного доступа в базы данных КОС и копирования конфиденциальной информации. Вместе с тем, мониторинг активности КОС показывает, что только за последние 4 месяца 2007 года (сентябрь-октябрь) система ИБ КОС «отбила» более 800 потенциальных АВК с неповторяющихся IP-адресов на КОС организации. Эти и другие многочисленные статистические данные убедительно свидетельствуют о правильности предложенных концептуальной и архитектурной моделей ИБ КОС.

СПИСОК ЛИТЕРАТУРЫ:

1. Сайт Московского технического университета экономики, статистики и информатики, http://www.mesi.ru
2. Отчет компании Computing Market Intelligence (UK) за 2005 год, доступен на сайте http://www.vnunet.com/vnunet/news/2126635/cost-malware-soars-166bn-2004
3. Отчет PGP корпорации за 2007 год, доступен на сайте http://www.pgp.com/newsroom/mediareleases/ponemon-us.html
4. Отчет ассоциации EDUCAUSE за 2007 год, доступен на сайте http://connect.educause.edu/Library/EDUCAUSE+Quarterly/CurrentIssuesSurveyReport/40026
5. Петренко С.А., Курбатов В.А. Политики информационной безопасности. – М.: Академия.